

VISIT...

LANZAROTE
Caliente.COM

17

Cyber Security of Substation Control and Diagnostic Systems

17.1	Introduction	17-1
17.2	Definitions and Terminology	17-2
17.3	Threats to the Security of Substation Systems.....	17-3
17.4	Substation Automation (SA) System Vulnerabilities.....	17-4
	Slow Processors with Stringent Real-Time Constraints • Real-Time Operating Systems that Preclude Security • Insecure Communications Media • Open Protocols • Lack of Authentication • Low Priority for Cyber Security • Lack of Centralized System Administration • Large Numbers of Remote Devices	
17.5	Measures to Enhance Cyber Security	17-6
	Protecting Substation Systems against Cyber Intrusion • Detecting Cyber Intrusion • Responding to Cyber Intrusion	
17.6	Devising a Security Policy	17-11
17.7	Future Measures	17-12
	Encryption • Secure Real-Time Operating Systems • Test Beds • Incident Reporting Sites • Intrusion Detection and Firewalls • Secure Recovery • Developing Standards • Security Policies and Procedures	
	References	17-15

Joseph Weiss

KEMA, Inc.

Martin Delson

KEMA, Inc.

17.1 Introduction

The traditional concerns of electric utilities about the security of their substation assets have centered on protecting the substation from physical threats, both natural and human threats. With the significant exception of countries with civil strife, the main human threats were believed to be from an individual disgruntled employee, angry customer, or politically motivated vandal. In the case of all of these threats, the malfeasant had to be within or physically close to the substation to cause any damage. Traditionally, providing physical security meant having fences, locked gates, security cameras, SCADA-monitored intrusion alarms, and occasional visits by utility staff.

In contemporary times, the nature and the magnitude of the threat to substation assets have changed. The nature of the threat has changed because the equipment to monitor and control substation devices is now frequently connected by communication lines to wide-area networks potentially accessible by the general public. (See, for example, the discussions in [Chapter 7](#), Substation Integration and Automation.) As a consequence, an individual seeking to damage utility assets can do so from places hundreds or thousands of kilometers distant as well as potentially impact multiple substations simultaneously.

TABLE 17.1 Traditional and Contemporary Threats to Utility Substations

Traditional Threats	Contemporary Threats
Threat is direct damage to the physical assets of the utility	Threat is damage to utility software systems, which may lead to damage to the physical assets
Threat is local	Threat originates from local or distant sources
Threat is from an individual	Threat may come from individuals, competitors, or well-funded and highly motivated organizations
An attack occurs at a single site	An attack may be unleashed simultaneously at many sites within many utilities and may be coordinated with cyber or physical attacks on other elements of key infrastructure
A successful attack causes immediate damage	A successful attack may be undetected, resulting in changes to utility software that lie dormant and are triggered to operate at some future time
A successful attack causes obvious damage	A utility may not know the nature of the damage to software caused by a successful attack
An attack is a single episode	As a result of an attack, software may be modified to cause continued damage
Restoration can safely take place after the attack	Since the attacker may still have access to the systems, restoration plans can be impacted

The magnitude of the threat has changed because organized and well-funded groups have publicly stated the goal of damaging elements of our critical infrastructure. Evidence shows that some organizations have been gathering information about public utilities in general, and specifically about SCADA technology [1]. Every day provides evidence of continuing probes of the electronic defenses of corporate computing networks. It is known that there have been episodes of probes specifically targeting the business systems of electric utilities [2]. However, because substations generally do not have firewalls or intrusion-detection systems, it is not possible to know if they are being targeted. There are several industry and government documents that have been issued on cyber security of SCADA systems and substation communications [3–10].

Table 17.1 summarizes the differences between the traditional threats to utility substation assets and contemporary threats. (The traditional threats have by no means evaporated; the new threats have to be seen as being in addition to, and not as a replacement of, the traditional threats.)

The previous chapter discussed protecting the physical security of the substation. This chapter addresses the nature of cyber threats, their potential to damage utility assets, and the means to protect against them, detect them when they do occur, and recover from them.

17.2 Definitions and Terminology

- **Cyber security:** Security (q.v.) from threats conveyed by computer or computer terminals; also, the protection of other physical assets from modification or damage from accidental or malicious misuse of computer-based control facilities.
- **Default password:** A password is a sequence of characters that one must input to gain access to a file, application, or computer system. A “default password” is the password that was implemented by the supplier of the application or system.
- **DNP3:** Distributed network protocol, a nonproprietary communications protocol (q.v.) designed to optimize the transmission of data-acquisition information and control commands from one computer to another [11].
- **Firewall:** A device that implements security policies to keep a network safe from unwanted data traffic. It can operate by simply filtering out unauthorized data packets based on their addresses, or it may involve more complex inspection of the sequence of messages to determine whether the communications are legitimate. A firewall can also be used as a relay between two networks, breaking the direct connection to outside parties.

- IDS: Intrusion detection system, a device that monitors the traffic on a communications line with the aim of detecting and reporting unauthorized users of the facilities. IDSs are programmed to identify and track specific patterns of activity.
- IEC: International Electrotechnical Commission, an international organization whose mission is to prepare and publish standards for all electrical, electronic, and related technologies.
- IED: Intelligent electronic device, any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers) [12].
- Port: A communications pathway into or out of a computer or networked device such as a server. Ports are often numbered and associated with specific application programs. Well-known applications have standard port numbers; for example, port 80 is used for HTTP traffic (Web traffic).
- Protocol: A formal set of conventions governing the format and relative timing of message exchange between two communications terminals; a strict procedure required to initiate and maintain communication [13].
- Remote access: Access to a control system or IED by a user whose operations terminal is not directly connected to the control systems or IED. Applications using remote access include Telnet, SSH, and remote desktop software such as pcAnywhere™, Exceed®, DameWare, and VNC. Transport mechanisms typical of remote access include dial-up modem, frame relay, ISDN, Internet, and wireless technologies.
- RTU: Remote terminal unit, the entire complement of devices, functional modules, and assemblies that are electrically interconnected to effect the remote station supervisory functions. The equipment includes the interface with the communication channel but does not include the interconnecting channel [14].
- Security: The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure [15].

17.3 Threats to the Security of Substation Systems

Investigations of threats to corporate computer hardware and software systems traditionally have shown that the greatest number of attacks come from internal sources [16]. Substation control systems and IEDs are different in that information about them is less well known to the general public. However, the hardware, software, architecture, and communication protocols for substations are well known to the utilities, equipment suppliers, contractors, and consultants throughout the industry. Often, the suppliers of hardware, software, and services to the utility industry share the same level of trust and access as the utility individuals themselves. Consequently, the concept of an insider is even more encompassing. A utility employee knows how to access the utility's computer systems to gather information or cause damage, and also has the necessary access rights (keys and passwords). The utility must protect itself against disgruntled employees who seek to cause damage as well as employees who are motivated by the prospect of financial gain. Computer-based systems at substations have data of value to a utility's competitors as well as data of value to the competitors of utility customers (e.g., the electric load of an industrial plant). Corporate employees have been bribed in the past to provide interested parties with valuable information; we have to expect that this situation will also apply to utility employees with access to substation systems. Furthermore, we cannot rule out the possibility of an employee being bribed or blackmailed to cause physical damage, or to disclose secrets that will allow other parties to cause damage.

A second potential threat comes from employees of suppliers of substation equipment. These employees also have the knowledge that enables them to access or damage substation assets. And often they have access as well. One access path is from the diagnostic port of substation monitoring and control equipment. (See [Chapter 7](#), Substation Integration and Automation.) It is often the case that the manufacturer

of a substation device has the ability to establish a link with the device for the purpose of performing diagnostics via telephone and modem (either via the Internet or else by calling the device using the public switched telephone network). An unscrupulous employee of the manufacturer could use this link to cause damage or gather confidential information. Additionally, an open link can be accessed by an unscrupulous hacker to obtain unauthorized access to a system. This has occurred frequently in other industries. Another pathway for employees of the utility or of equipment suppliers to illicitly access computer-based substation equipment is via the communications paths into the substation. Ensuring the security of these communications paths is the subject of Sections 8 and 10 of [Chapter 15](#), Substation Communications.

A third threat is from the general public. The potential intruder might be a hacker who is simply browsing and probing for weak links or who possibly wants to demonstrate his prowess at penetrating corporate defenses. Or the threat might originate from an individual who has some grievance against the utility or against society in general and is motivated to cause some damage. The utility should not underestimate the motivation of an individual outsider or amount of time that someone might dedicate to investigating vulnerabilities in the utility's defenses.

A fourth threat is posed by criminals who attempt to extort money (by threatening to do damage) or to gain access to confidential corporate records, such as maintained in the customer database, for sale or use.

The fifth, and arguably the most serious, threat is from terrorists or hostile foreign powers. These antagonists have the resources to mount a serious attack. Moreover, they can be quite knowledgeable, since the computer-based systems that outfit a substation are sold worldwide with minimal export restrictions, and documentation and operational training is provided to the purchaser. The danger from an organized hostile power is multiplied by the likelihood that an attack, if mounted, would occur in many places simultaneously and would presumably be coupled with other cyber, physical, or biological attacks aimed at crippling the response capabilities.

17.4 Substation Automation (SA) System Vulnerabilities

Conventional computer systems have been the object of a wide variety of cyber attacks. These include an exploitation of programming errors in operating systems and application software, guessing or cracking user passwords, taking advantage of system installations that leave extraneous services and open ports open to attack, and improperly configured firewalls that do not exclude unauthorized communications. In addition to manifesting these common vulnerabilities, the control and diagnostic systems in substations have a number of special vulnerabilities to their cyber security.

This section will not attempt to discuss the manifold vulnerabilities of conventional computer systems, which are well documented in other sources [17]. Instead, this section describes some of the characteristics of substation control and diagnostic systems that give rise to special vulnerabilities. Section 17.5 will then cover how the user can reduce the threats to cyber security and describe some of the characteristics of substation systems that make it difficult to apply conventional protective measures.

17.4.1 Slow Processors with Stringent Real-Time Constraints

One way to strengthen the privacy and authenticity of messages transmitted across insecure channels is to use encryption. The encryption techniques that are currently approved by the U.S. National Institute of Standards and Technology use block encryption [18]. This encryption technique is too resource-intensive for most current IEDs and many existing SA systems. Many substation communications channels do not have sufficient bandwidth for the transmission of longer block-encrypted messages. Furthermore, vendor testing has demonstrated that utilizing existing encryption technology would significantly slow down processing and inhibit timing functions. The remote terminal units (RTUs) and intelligent electronic devices (IEDs) in substations in some cases use early microprocessor technology. They have limited

memory and often have to meet stringent time constraints on their communications. It is often not feasible to require that these RTUs or IEDs enhance communications security by encrypting the data messages because their microprocessors do not have the processing capability to support the additional computational burden.

17.4.2 Real-Time Operating Systems that Preclude Security

Another security risk is posed by the design of the real-time operating systems that are embedded within many IEDs. At the present time, the suppliers of these embedded operating systems have not been faced with the need to meet the requirements for secure communications. Their software systems have been designed to operate in an environment poor in computing resources but where there is a need for deterministic response to events. Such systems are configured to prioritize the execution of tasks and communications, but not to implement information security policies. The embedded operating systems cannot make the requisite calls to authenticate the other party, encrypt data before sending it, and decrypt it upon reception.

17.4.3 Insecure Communications Media

The data messages that substation IEDs exchange with the outside world are often transmitted over media that are potentially open to eavesdropping or active intrusion. Dial-in lines are common; IEDs will accept phone calls from anyone who knows or discovers their phone number. Many IEDs are IP (Internet protocol)-enabled, i.e., they can be addressed by computers connected to the Internet.

In addition, much of the data traffic to and from a substation goes over wireless networks. (See [Chapter 15](#), Substation Communications.) Intruders with the proper equipment can record and interpret data exchanges and can insert their own messages to control power system devices. Other data traffic goes over leased lines, passing through telephone-company switching centers where they are subject to monitoring or interference. In this latter case, the security of substation operations can be no better than the security of the switching center of the telephone company.

Furthermore, the electronic equipment at substations frequently employs remote desktop applications (such as X-Terminal, pcAnywhere™, and Exceed®) that are specifically designed to allow users at remote locations to interact with the equipment as if they were present in the substation and directly at the local keyboard. There are many vulnerabilities to these remote-access programs. Substations are seldom configured with firewalls to help safeguard the systems from intrusion, and intrusion detection systems are not available for substation environments to alert the system operator when intrusions occur. (See Section 17.5.2.)

17.4.4 Open Protocols

The communications protocols used most frequently within substations are well known. For communications among IEDs, Modbus, Modbus-Plus, and DNP3 are the most frequently used protocols. These protocols are well documented and used worldwide. Many protocols have been used for communications between the substation and the utility's control center. In the past, these protocols were often vendor specific and proprietary, but in recent years the majority of implementations have been with IEC 60870-5 (in Europe), DNP3 (in North America), and to a much more limited extent, IEC 60870-6 TASE.2 (also called IEC 60870-6 TASE.2). These protocols are all nonproprietary, well documented, and available to the general public. Security was not a factor when these protocols were designed, and they currently contain no features to ensure the privacy or authenticity of the data transmitted.

Moreover, devices called "RTU test sets" are commercially available. An RTU test set is typically a portable device with a communications port that interfaces with an RTU or IED. The test set has a user interface that interprets the messages being sent to and from an RTU or an IED and that allows the user to define and issue commands to the substation device. Tabletop demonstrations have shown that an

intruder can patch into the communications channel to a substation and use a test set to operate devices at the substation. Depending on how the protocol has been implemented in the SCADA system, it is possible for an intruder to operate a device using a test set without the SCADA system recognizing the intrusion.

17.4.5 Lack of Authentication

Communication protocols in current use do not provide a secure means for data-exchanging systems to be certain of each other's identity. Intruders who gain access to a communications line to a controllable device can execute a control as if they were an authorized user. Intruders could also mimic a data source and substitute invalid data. In most cases, the program receiving the data performs very little effective data-validity checking to detect this kind of interference.

17.4.6 Low Priority for Cyber Security

Another characteristic of SA systems that adds to their vulnerability to cyber intrusion is managerial rather than technical. Owners of the systems often do not assign a high priority to cyber security. Utilities often zealously guard their operational systems from perceived interference from corporate information technology (IT) staff. Yet it is the corporate IT staff that often is most aware of the cyber threats to computer systems and most knowledgeable about the ways to protect these systems. Such knowledge is less frequently present among the staff responsible for SA systems.

Maintenance responsibility for substation equipment is often divided among different staff personnel, e.g., relay technicians for relay IEDs, substation technicians for transformer-monitoring IEDs, and communications technicians for RTUs. There is often no single individual with authority to oversee the cyber security of these various systems. As a corollary, there seldom are sufficient resources dedicated to providing security. Finally, because the subject of cyber security has, until recently, not received much attention, security-related policies and procedures very often need to be developed, approved, and put into practice.

17.4.7 Lack of Centralized System Administration

Unlike the IT domain, where there is a central system administrator to designate and track authorized users, SA system users are often their own system administrators. As such, they have the authority to perform all security functions. This often results in providing access to SA systems for personnel who have no reason to have such access. Additionally, the system administration function allows what is known as "root access." A user with root access has access to all critical functions, including assigning passwords, assigning log-in IDs, configuring the system, and adding or deleting software. These can lead to significant cyber vulnerabilities.

17.4.8 Large Numbers of Remote Devices

A typical utility has from several dozen to several hundred substations at geographically dispersed locations, and each automated substation typically has many IEDs. Therefore, there is a high cost to implement any solution that requires upgrading, reprogramming, or replacing the IEDs.

17.5 Measures to Enhance Cyber Security

The principles for enhancing the cyber security of control and diagnostic systems at substations are the same as those for other corporate computer systems: (1) prevent cyber intrusion where you can; (2) detect intrusion where it could not be prevented; (3) recover from an intrusion after it was detected; and (4) improve the preventive measures on the basis of experience.

17.5.1 Protecting Substation Systems against Cyber Intrusion

There are two avenues of potential cyber intrusion to the computer-based equipment in a substation: those originating from the users on the corporate network and those originating outside. These are treated in separate sections below.

17.5.1.1 Cyber Intrusion from Inside the Corporate Network

To the extent that substation control and monitoring systems are connected to a utility's corporate wide-area network, a large potential threat to these systems is derived from unauthorized users on the corporate network. Consequently, the first step in securing substation assets should be to ensure that the corporate network is made as secure as possible. The important measures are well known. They include the following:

- Removing all default user IDs and default passwords on installed systems
- Ensuring that all accounts have strong passwords
- Closing unneeded ports and disabling unneeded services
- Installing security patches from software suppliers in a timely manner
- Removing all sample scripts in browsers
- Implementing firewalls with carefully thought-out rules to exclude all unauthorized traffic
- Implementing intrusion detection systems and then logging and investigating all suspicious activity

The details of these and further measures to protect the corporate network are the subject of much active discussion elsewhere [19, 20] and will not be covered in this volume.

Even when measures are taken to enhance the cyber security of the corporate network, it would be foolish to assume that no intrusion is possible. Therefore, additional measures should be taken to further protect substation systems from successful penetrations onto the corporate network. These measures will also help protect substations from malevolent activity from employees who have access to the corporate network.

- The most important measure is one of the simplest, i.e., ensuring that all default passwords have been removed from all substation systems and that there are no accounts without any password. (This may not be possible, however, if the equipment supplier has “burned-in” the default password into the system firmware.)
- A password policy should be implemented to ensure that user passwords are not easily guessable. However, passwords that are difficult to guess are also difficult to remember. Users who post their passwords on the terminal of the system being protected defeat the purpose of the password. Users should be given instruction in ways to generate “difficult” passwords that they can remember without difficulty.
- A procedure should be in place to immediately terminate a password as soon as its owner leaves employment or changes job assignments.
- Different sets of privileges should be established for different classes of users. For example, some users should be allowed only to view historical substation data. Other users might be permitted to view only real-time data. Operators should be given only control privileges, and relay engineers should be given only the authority to change relay settings.
- The utility might consider requiring a stricter measure of authentication of the user before permitting access to a substation system. For example, the utility might want to consider requiring presentation of a smart card or instituting biometric identification (such as a personal fingerprint reader) for users desiring access to a system. The costs of purchasing the hardware to implement these protective measures is not high, but the administrative costs might make such measures impractical. As is often the case with issues of security, the utility must weigh the costs of the measure against the value of the asset being protected and the perceived risk of damage.

17.5.1.2 Cyber Intrusion from Outside the Corporate Network

The possibility of intrusion into the substation by outsiders gaining direct access to substation devices through unprotected communications channels raises new challenges to the cyber security of substation systems. There are two main communication paths into the substation that are potential targets for eavesdropping or intrusion: the SCADA communication lines and dial-up lines to IEDs.

17.5.1.2.1 SCADA Communication Lines

The SCADA communication line is the communications link between the utility's control center and the RTU at the substation. This line carries real-time data from substation devices to the utility dispatchers at the control center, and it controls messages from the dispatchers back to the substation. (For substations equipped for substation automation, a data concentrator or a substation-automation host processor will play the role of the RTU in sending substation data to the control center and in responding to the dispatcher's control commands.)

A variety of media are used to connect the substation RTU with the control center: power line, leased lines, microwave, multiple-address radio, satellite-based communications, fiber-optic cable, etc. The topic is discussed in detail in [Chapter 15](#), Substation Communications. It is quite common for communications from control center to substation to use different media along different segments of the path. Some of these media, especially the wireless ones, are open to eavesdropping or active intrusion. At least one case has been reported in which an intruder used radio technology to commandeer SCADA communications and sabotage the system (in this case, a wastewater treatment facility) [21]. Of the many alternatives, using fiber optics offers the most security against potential intruders to SCADA communications. Refer to Sections 8 and 10 of Chapter 15 for a thorough discussion of measures to protect SCADA communications.

17.5.1.2.2 Dial-Up Lines to IEDs

The other path to substation control and monitoring devices is via dial-up lines directly to intelligent electronic devices (IEDs). As discussed in [Chapter 7](#), Substation Integration and Automation, IEDs are devices that intrinsically support two-way communications. IEDs are frequently configured so a user can dial up the IED. Once the user has logged on to the IED, the user can use the connection to:

- Acquire data that the IED has stored
- Change the parameters of the IED (e.g., the settings of a protective relay)
- Perform diagnostics on the IED
- Control the power system device connected to the IED (e.g., operate a circuit breaker)

These dial-up lines can offer a simple path for a knowledgeable intruder into the substation. There are three lines of defense that a utility can take: (a) strengthen the authentication of the user, (b) encrypt communications with the IED, or (c) eliminate the dial-up lines.

17.5.1.2.2.1 Strengthening the Authentication of the User — “Authentication” refers to the process of ensuring that the prospective user of the IED is the person he claims to be. As the very first step, the utility should ensure that the default passwords originally supplied with the IEDs are changed and that a set of strong passwords are implemented.

A simple second step would be to confirm that the telephone call comes from a recognized source. For this purpose, it is not sufficient to get the user ID of the caller and confirm that it is on an approved list. Hackers are often familiar with telephone technology, and the caller ID can be changed or disguised. A more secure approach would be for all dial-in calls to be received by a dial-back device at the substation (also known as a call-back device.) The device receives the incoming call, requires that the caller enter a user ID and password, searches an internal list for the telephone number that the call should be made from, terminates the incoming call, and dials back the caller at the phone number found in the list. In essence, the incoming call is replaced by an outgoing call. It should be noted that the use of dial-back is not foolproof, however. According to one source [22]:

There are several ways an intruder can defeat the protection offered by a dial-back modem. For example, if the same modem and line are used for returning the call to the user, the intruder may be able to maintain control of the line while fooling the modem into acting as though the user had hung up after the original call. The modem would then place the return call, but the intruder's equipment would be mimicking the operation of the telephone system and the return call would be connected to the intruder's modem. Alternatively, the intruder could modify the telephone switch setup to direct the return call to the intruder's telephone number regardless of the pre-arranged number stored in the modem.

To defend against this threat, the report recommends that the utility consider the use of a separate line for the call back. The telephone switch must also be carefully protected, since the security of the substation depends on the integrity of the telephone switch.

17.5.1.2.2.2 Encrypting Communications — A second approach to enhancing the security of communications to IEDs would be to encrypt the messages between the user and the IED. Encryption could help ensure that only users in possession of the secret key would be able to interpret data from the IED and change IED parameters. (As an alternative to encryption, the utility also has the option of embedding a “secure hash” in messages. This technique entails computing a special code that is added to the message. The code is a function of the contents of the message and of a secret key that should be known only to the user and the IED. Computing a “secure hash” is much less computationally intensive than encrypting the whole message.)

At the time of publication, encrypting the communications to IEDs does not appear to be practical. In IED design, the two paramount factors are performance and cost. The high computational requirements of processors to implement some encryption schemes make encryption impractical for the low-performance microprocessors currently used in many IEDs. Moreover, the suppliers of IEDs are reluctant to add functions that will raise the cost. In addition, the standards community has not yet agreed upon a unified approach to encryption. Consequently, at the current time, it would take a special effort on the part of a utility to encrypt messages to and from IEDs. The cost of such an effort would make this infeasible in most existing implementations.

Nevertheless, there are active developments along several fronts that may cause this situation to change. Higher performance microprocessors are being manufactured at ever-lower cost, reducing the cost and performance penalties of encryption. In addition, several groups are making progress in defining encryption standards for the communication protocols used in substations, including IEC Technical Committee 57 Working Groups 7 and 15 and the DNP Users Group. The IEC 61850 protocol is based upon international standard communication profiles, which include provisions for communications security. While the final security architecture has not been defined at the time of this writing, 61850 includes provisions for security features at the application layer and in the protocol stack that will be added to the profile in its final form. Once the industry has agreed upon a standard technique for encrypting messages, the IED manufacturers can plan on realizing economies of scale. We can be fairly confident that if there is a demand for encryption of IED communications, and industry-wide agreement on the approach, then the IED manufacturers will find it possible to embed the algorithm in the processor of the IEDs at little incremental cost.

An alternative that can be considered in the meantime is the use of an external device that is interposed between the dial-in modem and the serial cable to the IED. Devices are commercially available that encrypt messages. (The encryption is done using a stream cipher, a technique that can operate while the message is in the process of being transferred.) Using such an in-line encrypting device provides the privacy and authentication of encryption at reasonable cost without requiring a change in the IED processor. The penalty in performance is the delay of a few bytes per message exchange. Adding an in-line encrypting device does add additional equipment to the substation, with the concomitant increase in complexity, impact on reliability, and additional administrative burden. However, this is not expected to be significant. It should be noted that the encryption does not validate the data. It assumes the data to be trusted and encrypts the data. If the data are corrupted prior to reaching the encryption device, corrupted data will be sent in an encrypted manner.

17.5.1.2.2.3 Eliminating the Dial-Up Lines — Another approach to securing the communications to IEDs would be to eliminate dial-up lines into the substation entirely. This approach is indeed being followed by several utilities that place a high value on cyber security.

Under this approach, all communications to the IEDs originate from within the secure network and are transmitted through and mediated by the data concentrator or substation host processor at the substation. The data concentrator or substation processor forwards the message to the appropriate IED and routes the response back to the original caller. (In the terminology of [Chapter 7](#), Substation Integration and Automation, these messages use “pass through” communications.) No communications to the substation are permitted that originate outside the secure utility network. Communications to the substation IEDs would be even more secure if, as suggested earlier, fiber-optic lines were used for substation communications.

The security of this approach is dependent, of course, on the success of the utility in preserving the security of its internal network. That issue is beyond the scope of this chapter.

17.5.2 Detecting Cyber Intrusion

One of the axioms of cyber security is that while it is extremely important to try to prevent intrusions into one's systems and databases, it is essential that intrusions be detected if they do occur. An intruder who gains control of a substation computer can modify the computer code or insert a new program. The new software can be programmed to quietly gather data (possibly including the log-on passwords of legitimate users) and send the data to the intruder at a later time. It can be programmed to operate power system devices at some future time or upon the recognition of a future event. It can set up a mechanism (sometimes called a “backdoor”) that will allow the intruder to easily gain access at a future time.

If no obvious damage was done at the time of the intrusion, it can be very difficult to detect that the software has been modified. For example, if the goal of the intrusion was to gain unauthorized access to utility data, the fact that another party is reading confidential data may never be noticed. Even when the intrusion does result in damage (e.g., intentionally opening a circuit breaker on a critical circuit), it may not be at all obvious that the false operation was due to a security breach rather than some other failure (e.g., a voltage transient, a relay failure, or a software bug).

For these reasons, it is important to strive to detect intrusions when they occur. To this end, a number of IT security system manufacturers have developed intrusion detection systems (IDS). These systems are designed to recognize intrusions based on a variety of factors, including primarily (a) communications attempted from unauthorized or unusual addresses and (b) an unusual pattern of activity. They generate logs of suspicious events. The owners of the systems then have to inspect the logs manually and determine which represent true intrusions and which are false alarms.

Unfortunately, there is no easy definition of what kinds of activity should be classified as “unusual” and investigated further. To make the situation more difficult, hackers have learned to disguise their network probes so they do not arouse suspicion. In addition, it should be recognized that there is as much a danger of having too many events flagged as suspicious as having too few. Users will soon learn to ignore the output of an intrusion detection system that announces too many spurious events. (There are outside organizations, however, that offer the service of studying the output of IDSs and reporting the results to the owner. They will also help the system owner to tune the parameters of the IDS and to incorporate stronger protective features in the network to be safeguarded.)

Making matters more difficult, most intrusion detection systems have been developed for corporate networks with publicly accessible Internet services. Very little research has been done to investigate what would constitute “unusual” activity in a SCADA environment. In general, SA and other control systems do not have logging functions to identify who is attempting to obtain access to these systems. Efforts are underway in the commercial arena and with the National SCADA test bed at DOE's Idaho National Engineering and Environmental Laboratory (INEEL) to develop intrusion-detection capabilities for control systems.

In summary, the art of detecting intrusions into substation control and diagnostic systems is still in its infancy. Until dependable automatic tools are developed, system owners will have to place their major efforts in two areas: (a) preventing intrusions from occurring and (b) recovering from them when they occur.

17.5.3 Responding to Cyber Intrusion

The “three Rs” of the response to cyber intrusion are recording, reporting, and restoring.

Theoretically, it would be desirable to record all data communications into and out of all substation devices. In that manner, if an intruder successfully attacks the system, the recordings could be used to determine what technique the intruder used to modify the system, and then close that particular vulnerability. Secondly, the recording would be invaluable in trying to identify the intruder. In addition, if the recording is made in a way that is demonstrably inalterable, then it might be admissible as evidence in court if the intruder is apprehended. However, due to the high frequency of SCADA communications, the low cost of substation communications equipment, and the fact that the substations are distant from corporate security staff, it may be impractical to record all communications.

In practice, although theoretically desirable, system owners will probably defer any attempts to record substation data communications until (a) storage media are developed that are fast, voluminous, and inexpensive, or (b) SCADA-oriented intrusion detection systems are developed that can filter out the nonsuspicious usual traffic and record only the deviant patterns. But even if the communications sequence responsible for an intrusion is neither detected nor recorded when it occurs, nevertheless it is essential that procedures be developed for the restoration of service after a cyber attack.

It is extremely important that the utility maintain backups of the software of all programmable substation units and documentation regarding the standard parameters and settings of all IEDs. These backups and documentation should be maintained in a secure storage, not normally accessible to the staff who work at the substation. It would appear advisable that these backups be kept in a location other than the substation itself to lower the amount of damage that could be done by a malicious insider.

After the utility concludes that a particular programmable device has been compromised (indeed, even if it just suspects a successful intrusion), the software should be reloaded from the secure backup. If the settings on an IED had been illicitly changed, the original settings must be restored. Unless the nature of the breach of security is known and can be repaired, the utility should seriously consider taking the device off line or otherwise making it inaccessible to prevent a future exploitation of the same vulnerability.

17.6 Devising a Security Policy

In order to put the recommendations of this chapter into practice, a utility should establish and implement a security policy. The policy for the cyber security of the systems in a substation should be a component of a larger plan for the cyber security of the entirety of a utility’s computer-based systems. (This is vitally important since, as was emphasized earlier, the largest vulnerability of the control and diagnostic systems at a substation arises through the connection of these systems to the corporate wide-area network and, through the corporate network, to the Internet and the outside world.)

The policy for the cyber security of a utility’s computer systems should also be correlated with a plan for ensuring the physical security of the utility’s assets. (Some of the components of a plan for cyber security will be very similar to the analogous plan for physical security.) The utility should consider the issues outlined below when devising the security policy. Further, more detailed suggestions about the elements of a cyber security plan can be found in many published sources [19, 20].

- Assets

What are the assets of the substation that the policy seeks to protect? (As a corollary, what assets are not protected by the policy?)

What level of protection should be given to each asset (device, control system, communications system, database)?

What must a user do or have to gain access to each asset?

- Threats

What are the threats to the security of the substation that the policy seeks to address? (Also, what threats are not addressed?)

What is the damage that can result from each of the threats?

What measures should be taken to protect against each threat? (Several alternatives may be considered.)

What should be done to test the protective measures that have been taken? (Should an outside organization be employed to probe for weaknesses?)

Who will monitor the changing nature of cyber threats and update the security policy accordingly?

- Threat detection

What measures will be taken to detect intrusion? (Should an outside party be employed to analyze intrusion records?)

What should be done if an intrusion is suspected?

Who should an intrusion be reported to?

What records should be kept?

- Incident response

What immediate steps should be taken in response to each type of incident?

What role will law enforcement play?

How will the incident be reported to regulatory agencies, reliability councils, or cyber incident recording centers?

What improvements must be made (to policy, to documentation, to training, etc.) as a result of lessons learned?

- Training and documentation

What are the training programs for security (general security awareness, access procedures, restoration procedures)?

What are the plans for practicing restoration, and how often will they be applied?

What are the plans for supporting manual operation if control systems suffer long-term damage?

Who will issue the documentation for the restoration procedures, and where will the documents be kept?

- Administration

Who has the ultimate responsibility for cyber security at the utility?

What are the responsibilities of each relevant job category?

What are the potential consequences for staff of a violation of policy?

How will compliance with the policy be monitored? (Should an outside organization be used?)

How will the security policy be revised?

- Software management

How will software updates be authenticated, tested, and installed?

How will security patches be tested and installed?

How will system backups be secured?

What are the rules for acceptable passwords?

17.7 Future Measures

It should be clear from the previous discussion that, at the time of publishing, the technology is not yet mature enough to ensure the cyber security of control and diagnostic systems at substations. To a certain extent, a utility will be forced to make do with halfway measures. It is not practical to eliminate all security

risks or to close all security vulnerabilities. The utility must evaluate what assets have the highest value and deserve the greatest protective effort.

Strenuous efforts are being taken in several areas to improve the defenses against cyber threats. It will be worthwhile for the utility to monitor these developments and update their security policies to take advantage of technological advances. (As was the case with the arms race, however, it must be anticipated that adversaries will develop new attack strategies as current vulnerabilities are closed; it is important that the utility monitor and respond to the changing nature of the threat as well.) This chapter describes some current developments that will make it easier to provide for the cyber security of substation systems, and it indicates where further work is needed.

17.7.1 Encryption

The various standards groups who are responsible for defining the protocols used in substation communications are actively working on defining the standards for encryption. Concurrently, IEDs are being manufactured with faster microprocessors and more memory, making it feasible to implement encryption in embedded processors. Furthermore, the channel capacity of communications lines to substations is growing, making the performance penalty for encryption less significant. As a result of these trends, it will soon be feasible to encrypt communications between control centers and substations. In addition, if there is demand for the function from the user community, it may be possible to implement encryption of communications among IEDs within a substation at acceptable cost. SCADA test beds at the DOE National Laboratories are identifying which security technology is appropriate for specific applications. It is conceivable that encryption may not be necessary.

17.7.2 Secure Real-Time Operating Systems

An ancillary, but important function is to develop real-time operating systems with security policies. This will enable calls to be made to authorize, authenticate the other party, and encrypt and decrypt data.

17.7.3 Test Beds

It is difficult for a utility, unaided, to discover all the security vulnerabilities in the various systems installed at a substation. In recognition of the need for a more concerted effort, the U.S. government has recently started to dedicate resources to investigate the security vulnerabilities of elements of the critical infrastructure. Several national laboratories have taken on the task of establishing the National SCADA Test Bed, where the SCADA systems in common use can be studied, their vulnerabilities discovered, and remedies implemented. It is expected that the role of the test beds will be expanded to include the control and diagnostic systems commonly used in substations.

17.7.4 Incident Reporting Sites

For several years, the CERT Coordination Center (CERT/CC), operated by Carnegie Mellon University, has served as a storehouse for reports of security incidents. CERT declares, "Our work involves handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training to help you improve security at your site."

The CERT Web site (<http://www.cert.org/>) has a form that allows the manager of a computer system or network to report a security incident. CERT also publishes an advisory of cyber security problems, which is e-mailed to a very large number of destinations. Utilities should be encouraged to make use of the CERT incident reporting service to report security incidents, and thereby inform others of common vulnerabilities. (CERT promises to keep the source of the information confidential.)

At the current time, the incidents maintained on the CERT database are almost entirely traditional computer problems; problems with SCADA and substation automation systems have not been identified

in their advisories. However, there have been many cases of intentional and unintentional cyber impacts on control systems in various industries, including electric power, although very few have been formally documented [23, 24]. These impacts range from design flaws and improper procedures to actual hacking. Impacts have ranged from minimal to environmental damage and even deaths. Consequently, there is a need to develop a similar service focusing on the cyber security incidents relating to real-time control systems at utilities and industrial process control systems.

17.7.5 Intrusion Detection and Firewalls

It is important to be able to reliably recognize an intrusion into substation computer systems and networks. Currently, almost all intrusion detection systems focus on traditional computer networks and have not been adapted for the special circumstances characterizing the systems found at substations. Work is currently in progress to use neural networks to define a “usual” state of activity and to recognize an intrusion by the change in the patterns. At the current time, these efforts have not yet been proven to be effective. It is hoped that these developments will prove successful and that intrusion detection systems appropriate for utility application will become available.

Firewalls can protect the network by limiting information from accepted addresses only. However, firewall technology is currently not capable of inspecting data packets and making go/no-go decisions on passing data to the control system. Consequently, all data that appear to be from an accepted address are passed. This becomes an issue because certain malformed UDP packets have been demonstrated to cause fault conditions in specific control systems [25].

17.7.6 Secure Recovery

If a computer-based system has been compromised, the process of restoring the system to its pristine state is lengthy, labor-intensive, and error-prone. It is especially difficult when the software has been modified since it was first installed. The utility must answer the difficult questions about when the system was compromised, and whether the software that is being restored perhaps contains the infected code. Developments that would allow a quick and reliable restoration of uninfected system software would be of great value to the operators of substation control and diagnostic systems.

17.7.7 Developing Standards

The IEEE Power Engineering Society (PES) standards have been developed for performance and not cyber security requirements. To rectify this oversight, on July 22, 2002, the IEEE PES Standards Coordinating Council created a task force to do the following:

- Survey all IEEE PES standards (both existing and those under development) for electronic security issues
- Survey legislative and regulatory electronic security rules that may affect IEEE PES standards
- Survey other IEEE and industry standards for electronic security sections that may affect IEEE PES standards

IEC Technical Committee 57 Working Groups 7 and 15 are addressing IEC 60870-6 TASE.2 (“ICCP”). ISA has recently established a new standards committee for process controls cyber security, ISA SP99. The Open Group’s Real-Time Security Forum is working on developing application programming interfaces (APIs) for including security policies in the kernel of real-time operating systems.

17.7.8 Security Policies and Procedures

Existing IT security policies and procedures have not addressed the unique aspects of substation automation and similar control systems. Security policies such as ISO-17799 [20] need to be modified in recognition of the unique characteristics of substation control and diagnostic systems.

References

1. Gellman, B., Cyber Attacks by Al Qaeda Feared, *Washington Post*, June 27, 2002.
2. Riptech, Internet Security Threat Report — Attack Trends for Q1 and Q2 2002, Riptech, July 2002.
3. Weiss, J., Information Security Primer, EPRI Report TR-100797, Electric Power Research Institute, Palo Alto, CA, Sep. 2001.
4. North American Electric Reliability Council (NERC), Process Controls System Security: Remote Access, NERC Guideline, Version 0.1, NERC, Washington, DC, Nov. 2002.
5. American Gas Association (AGA), Field Communications Security Policy for the Gas Utility Operations Networks (SCADA), Version 0.5a, Washington, D.C., Apr. 2002.
6. Department of Energy, 21 Steps To Improve Cyber Security of SCADA Networks, USDOE, Washington, DC, Sep. 2002.
7. The President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, Sep. 2002.
8. Report for Congress, Critical Infrastructure Remote Control Systems and the Terrorist Threat, Order Code RL31534, Aug. 2002.
9. Fitzpatrick, G. and Weiss, J., Control systems: the weak link in infrastructure protection, *Platt's Energy Bus. Technol.*, Sep. 2002.
10. Weiss, J., Testimony to the U.S. House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Control System Cyber Security — Maintaining the Reliability of the Critical Infrastructure, July 2002.
11. DNP Users Group, A DNP Protocol Primer, available on-line at http://www.dnp.org/files/dnp3_primer.pdf.
12. Institute of Electrical and Electronics Engineers, IEEE Standard Definition, Specification and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control, IEEE Std. C37.1-1994, IEEE, Piscataway, NJ, 1994.
13. Institute of Electrical and Electronics Engineers, IEEE Standard Dictionary of Electrical and Electronics Terms, ANSI/IEEE Std. 100-1984, 3rd ed., IEEE, Piscataway, NJ, 1984, p. 605.
14. Institute of Electrical and Electronics Engineers, IEEE Standard Dictionary of Electrical and Electronics Terms, ANSI/IEEE Std. 100-1984, 3rd ed., IEEE, Piscataway, NJ, 1984, p. 769.
15. Institute of Electrical and Electronics Engineers, IEEE Standard Dictionary of Electrical and Electronics Terms, ANSI/IEEE Std. 100-1984, 3rd ed., IEEE, Piscataway, NJ, 1984, p. 811.
16. Computer Security Institute, Seventh Annual Computer Crime and Security Survey, Computer Security Institute, San Francisco, Apr. 2002.
17. SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities, available on-line at <http://www.sans.org/top20.htm>.
18. National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards, Publication FIPS 140-2 Annex A, NIST, Gaithersburg, MD, May 25, 2001.
19. Allen, J. H., *CERT Guide to System and Network Security Practices*, Addison-Wesley, Reading, MA, 2001; available on-line at <http://www.cert.org/security-improvement/>.
20. International Standards Organization, International Security Standard, ISO-17799, ISO, Geneva.
21. Green, G., Hacker Jailed for Sewage Sabotage, *Courier-Mail* (Brisbane, Australia), Nov. 1, 2001.
22. Electric Power Research Institute, Information Security Guidelines for Transmission and Distribution Systems, draft unpublished report to J. Weiss, Stan Klein Associates, EPRI, Palo Alto, CA, Oct. 2000.
23. National Transportation and Safety Board, Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999, Report PAR-02/02 NTIS PB2002-916502, NTSB, Washington, DC.
24. Byers, E., Protect That Network: Designing Secure Networks for Industrial Control, paper presented at IEEE Pulp and Paper Technical Conference, Seattle, WA, June 1999.
25. Byres, E., demonstration of SCADA and process control systems, presented at KEMA Consulting Conference on Cyber Security, Vancouver, BC, 2002.